PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-045195
(43)Date of publication of application : 16.02.1999

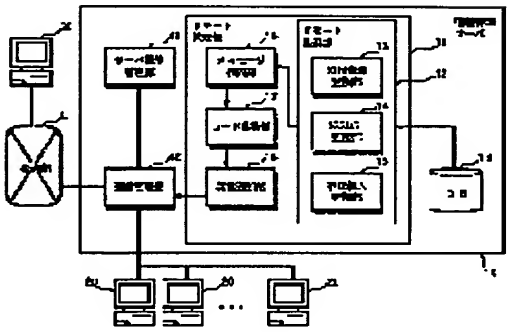
(51)Int.CI. G06F 11/30
G06F 13/00

(21)Application number : 09-202016
(22)Date of filing : 28.07.1997

(71)Applicant : N T T DATA:KK
(72)Inventor : YAMANAKA TOMOYUKI

(54) COMPUTER SYSTEM, ABNORMALITY DETECTOR AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a computer system for grasping trouble, which occurs at an information managing server to be a managing object, without remote operation from the outside.
SOLUTION: An information managing server 10 is provided with a system resource monitoring part 13 for preparing a notice message when the remaining storage capacitance of a DB 19 gets less than a reference capacitance, system error monitoring part 14 for monitoring a log and preparing a notice message when any abnormality is detected, and illegal invasion monitoring part 15 for comparing a process group under working with a process group at normal time and preparing a notice message when any abnormality is detected. These notice messages are automatically transmitted from the information managing server 10 to a system control managing server 30 by an electronic mail function. Thus, the trouble at the information managing server 10 can be easily grasped by the system control managing server 30.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

コンピュータシステム、異常検出装置及び記録媒体

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－45195

(43)公開日　平成11年(1999)２月16日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	11/30		Ｇ０６Ｆ	11/30	Ｄ
	13/00	３５１		13/00	３５１Ｇ

審査請求　未請求　請求項の数６　ＯＬ　（全９頁）

(21)出願番号　特願平9－202016

(22)出願日　平成９年(1997)７月28日

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号

(72)発明者　山中　智之
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

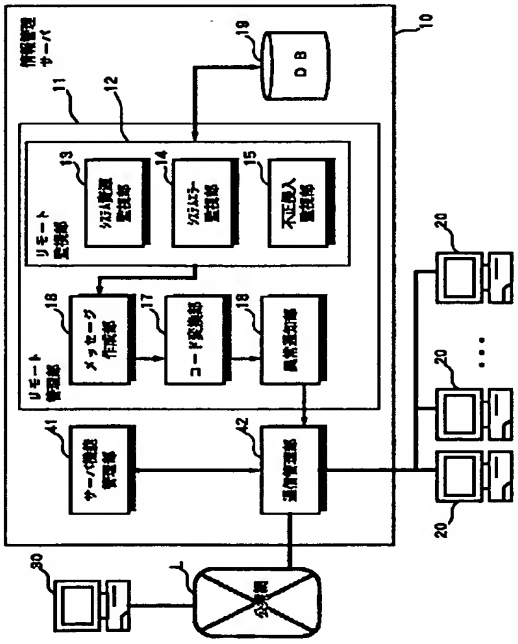
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　コンピュータシステム、異常検出装置及び記録媒体

(57)【要約】

【課題】　管理対象となる情報管理サーバで発生した不具合を外部から遠隔操作することなく把握できるようにしたコンピュータシステムを提供する。

【解決手段】　情報管理サーバ１０に、ＤＢ１９の記憶容量の残量が基準量以下になった場合に通知メッセージを作成するシステム資源監視部１３と、ログを監視して異常検出時に通知メッセージを作成するシステムエラー監視部１４と、稼働中のプロセス群と正常時のプロセス群との比較を行い、異常検出時に通知メッセージを作成する不正侵入監視部１５とを設ける。これらの通知メッセージは、電子メール機能により、情報管理サーバ１０から自動的にシステム統括管理サーバ３０に送信されるようにする。これにより、システム統括管理サーバ３０で容易に情報管理サーバ１０の不具合を把握できるようになる。



【特許請求の範囲】

【請求項１】　第１コンピュータ装置と、この第１コンピュータ装置に通信回線を通じて接続された第２コンピュータ装置とを備え、第２コンピュータ装置で第１コンピュータ装置の遠隔監視を行うコンピュータシステムにおいて、

前記第１コンピュータ装置が、

自装置における異常の有無を周期的に監視する監視手段と、

前記第２コンピュータ装置宛の電子メールを作成する手段とを備え、前記監視手段が異常を検出する毎に当該異常に関する情報を表す電子メールを作成して前記第２コンピュータ装置に通知することを特徴とするコンピュータシステム。

【請求項２】　前記監視手段は、

自装置がアクセスする記憶装置の残り容量を監視してその残り容量が予め設定された基準量以下となった場合に異常状態を表す検出情報を作成する資源監視手段、

自装置の稼働状況を表す履歴情報の変化状態を監視してその変化レベルが予め設定された通知レベルを超える履歴情報を検出したときに異常状態を表す検出情報を作成する履歴情報監視手段、

自装置における稼働中のプロセス群を予め設定された必要プロセス群情報と不要プロセス群情報とに基づいて特定し、特定したプロセス群に前記必要プロセス群情報及び不要プロセス群情報中に含まれないプロセス或いは不足するプロセスがあるときに異常状態を表す検出情報を作成するプロセス監視手段、

前記記憶装置に記憶された電子情報の識別子を予め保持した識別情報と比較し、前記識別子が前記識別情報に合致しない場合に異常状態を表す検出情報を作成するする識別情報監視手段の、少なくとも一つを周期的に起動し、それぞれ検出情報が作成されたときに前記電子メールを作成することを特徴とする請求項１記載のコンピュータシステム。

【請求項３】　前記監視手段は、前記作成された検出情報を所定のＳＭＴＰ対応コードに変換して前記電子メールを作成することを特徴とする請求項２項記載のコンピュータシステム。

【請求項４】　自装置がアクセスする記憶装置の残り容量を監視してその残り容量が予め設定した基準量以下となった場合に異常状態を表す検出情報を作成する資源監視手段、

自装置の稼働状況を表す履歴情報の変化状態を監視してその変化レベルが予め設定されたレベルを超える履歴情報を検出したときに異常状態を表す検出情報を作成する履歴情報監視手段、

自装置における稼働中のプロセス群を予め設定された必要プロセス群情報と不要プロセス群情報とに基づいて特定し、前記稼働中のプロセス群に前記必要プロセス群情報及び不要プロセス群情報中に含まれないプロセス或いは不足するプロセスがあるときに異常状態を表す検出情報を作成するプロセス監視手段、及び、

前記記憶装置に記憶された電子情報の識別子を予め保持した識別情報と比較し、前記識別子が識別情報に合致しない場合に異常状態を表す検出情報を作成する識別情報監視手段のいずれかを含み、さらに、

前記検出情報のいずれかが出力されたときに所定形式の電子メールを作成して外部装置に提示する手段と、

を備えてなる異常検出装置。

【請求項５】　前記履歴情報監視手段は、初期稼働時に取得した履歴情報を初期履歴情報として保持し、次回以降の履歴情報が更新された場合に、前記初期履歴情報と前記更新された履歴情報との差分による履歴情報を新たな初期履歴情報として保持するように構成されることを特徴とする請求項４記載の異常検出装置。

【請求項６】　記憶装置を具備したコンピュータ装置が読み取り可能なプログラムを記録して成る記録媒体であって、

前記プログラムが、

前記記憶装置の残り容量を監視してその残り容量が予め設定した基準量以下となった場合に異常状態を表す検出情報を作成する処理、

装置稼働状況を表す履歴情報の変化状態を監視してその変化レベルが予め設定されたレベルを超える履歴情報を検出したときに異常状態を表す検出情報を作成する処理、

稼働中のプロセス群を予め設定された必要プロセス群情報と不要プロセス群情報とに基づいて特定し、前記稼働中のプロセス群に前記必要プロセス群情報及び不要プロセス群情報中に含まれないプロセス或いは不足するプロセスがあるときに異常状態を表す検出情報を作成する処理、及び、

前記記憶装置に記憶された電子情報の識別子を予め保持した識別情報と比較し、前記識別子が識別情報に合致しない場合に異常状態を表す検出情報を作成する処理、の少なくとも一つの処理を前記コンピュータ装置に周期的に繰り返し実行させるものであることを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば広域ネットワークに接続された複数のコンピュータ装置からなるコンピュータシステムにおいて、各コンピュータ装置の異常の有無を周期的に自動検出して管理者に実時間で通知することによって、各コンピュータ装置の信頼性向上を図る手法に関する。

【０００２】

【従来の技術】近年、インターネットに代表される大規模かつ高速な広域ネットワークの普及等により、多様な

形態で複数の利用者に情報を提供するコンピュータシステムの開発が進められている。これらのコンピュータシステムでは、障害発生に伴うシステム全体の効率低下や、システムへの不正侵入者に対する機密保護等を考慮した、高信頼のシステム構築及びシステム運用管理が望まれている。通常、広域ネットワークを介して構築されたコンピュータシステムでは、クライアント・サーバシステム型の通信形態が採用されており、利用者は、クライアント側となるコンピュータ装置からアクセス用インタフェースを使用して、サーバにアクセスし、所望の電子情報を取得している。このようなコンピュータシステムでは、例えば、WWW（World Wide Web）サーバ、ＤＮＳ（Domain Name Server）、Ｐｒｏｘｙサーバ等、特有な処理を担当する各サーバを広域ネットワーク上に分散配置して利用者への情報提供を行っている。

【０００３】これらの各サーバにおいて、異常発生に伴うシステム障害の原因を検出するためには、システム管理者等が該当サーバにアクセスして、ＯＳ（オペレーティングシステム）や各種アプリケーションの稼働に伴う多様なシステムメッセージを時刻毎に記録したイベントログ等の履歴情報（以下、ログ）の内容を検証するのが一般的であり、ログにおける異常の有無を確認してから障害への対処を行っている。また、システム運用に関する必要なプロセスは、サーバ毎にある程度決まっているため、当該プロセスの消失、及び不要なプロセスの発生等を監視することで、迅速にシステム障害、或いは部分障害の検出に対処している。

【０００４】上述のクライアント・サーバシステム型におけるサーバ側のコンピュータ装置には、例えば、ＯＳ／ＵＮＩＸを搭載したワークステーション（以下、ＵＮＩＸマシン）等が多く採用されている。これは、ＵＮＩＸがＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）ベースの通信管理に最適な環境を提供していることが主な理由である。

【０００５】一方、クライアント側に採用されるコンピュータ装置は、ＵＮＩＸマシンと比較して低価格のＰＣ（パーソナルコンピュータ）が主流である。しかし、このＰＣにおいても、例えば、Microsoft社のＷｉｎｄｏｗｓＮＴ等に見られるような通信管理が強化されたＯＳの出現に伴い、サーバ側のコンピュータ装置として採用されるようになってきている。

【０００６】この場合の使用形態としては、例えば、比較的小規模な複数のクライアントに対して通信管理を行うサーバをＰＣで構築する。以下、ＰＣで構築したサーバをＰＣサーバとする。また、複数のクライアント毎に同様なＰＣサーバを構築するとともに、これらのＰＣサーバに対して、統合した管理を行うＮＯＣ（NetworkOperations Center）のようなセンターサーバを、ＵＮＩＸマシン等で構築してシステム全体の管理運用を行う。また、ＰＣサーバにシステム障害等が発生した場合には、ＮＯＣから該当するＰＣサーバに対してリモートアクセスを行い、障害への対処を行うように構成されている。

【０００７】

【発明が解決しようとする課題】しかし、上述のようにＰＣサーバとセンターサーバとを使用してコンピュータシステムを構築した場合には、以下のような問題がある。

（１－１）センターサーバによるＰＣサーバのログの取得、検査は、該当するＰＣサーバに対して公衆網を介したリモートアクセスにより行われるため、一般にその作業が煩雑となる。

（１－２）センターサーバまたはＰＣサーバでは、動作中のプロセス一覧を得ることはできるが、それらの必要・不要の判定は人間が行わなければならない。

（１－３）センターサーバは、ＰＣサーバにおけるシステムの異常、障害等の発生に対処するために定期的なメンテナンスを行う必要がある。

（１－４）ＰＣサーバに具備または接続されるディスク等の記憶装置の容量減少に伴って当該ＰＣサーバの動作に悪影響を与える場合に、その悪影響の原因の検出ができない。

（１－５）例えば、システムにおけるセキュリティの弱点（セキュリティ・ホール）が公衆網を介して侵入者に発見され、不正に侵入された場合には、プロセスの状態から当該侵入行為の検出が可能である。これは、侵入者がシステムにおいて、何らかのアプリケーションを起動させれば必ず新たなプロセスが発生するという理由に依るが、ＰＣサーバにおいては、不要プロセスの発生や、必要プロセスの消失等に関する検出ができない。

（１－６）センターサーバでは、ＰＣサーバが、再度起動不可能となるようなシステム障害の発生原因を究明する場合、当該障害に至るまでの経緯を取得（把握）することができない。

【０００８】一方、ＰＣに依存する以下のような問題もある。

（２－１）例えばＷｉｎｄｏｗｓＮＴのようなＰＣ環境では、ＵＮＩＸマシンと比較して汎用性の高い電子メールシステムが提供されていない。

（２－２）ＷｉｎｄｏｗｓＮＴのＰＣ環境では、漢字コードにＳ－ＪＩＳコードが使用されており、Ｓ－ＪＩＳコードでは、ＴＣＰ／ＩＰの電子メール交換プロトコルであるＳＭＴＰ（Simple Mail Transfer Protocol）を使用することができない。

（２－３）Microsoft社のＯＳで広く採用されているＤＬＬ（Dynamic Link Library）は、プログラムが実行される場合にはアプリケーションと結合し、必要がなくなればアンロードされるように構成されているが、WWW環境のＩＩＳ（Internet Information Server）においては、サーバのセキュリティ・ホールとなるフィルタＤＬＬのパスの不要な変更を監視できない。

（２－４）センターサーバでは、ＰＣサーバの動作を設定するパラメータの変更処理等を公衆網を介したリモート環境で動的に制御できない。

【０００９】そこで、本発明の課題は、例えばＰＣサーバやセンターサーバのような管理対象コンピュータ装置とこのコンピュータ装置の遠隔監視を行う管理コンピュータ装置とを含むコンピュータシステムにおいて、管理対象コンピュータ装置で生じている不具合を管理コンピュータ装置側から遠隔操作することなく容易に把握できるようにすることにある。具体的には、管理対象コンピュータ装置において、記憶容量の減少や稼働状況の不具合等が発生したときにこれを管理コンピュータ装置に速やかに通知し、また、管理対象コンピュータ装置において重大な異常が検出された場合には管理コンピュータ装置でそれを把握して、管理対象コンピュータ装置が故障に至った経緯を解析できるようにすることにある。本発明の他の課題は、上記コンピュータシステムの実施に適した異常検出装置、及び当該異常検出装置を汎用のコンピュータ装置で実現するための記録媒体を提供することにある。

【００１０】

【課題を解決するための手段】上記課題を解決する本発明のコンピュータシステムは、第１コンピュータ装置と、この第１コンピュータ装置に通信回線を通じて接続された第２コンピュータ装置とを備え、第２コンピュータ装置で第１コンピュータ装置の遠隔監視を行うコンピュータシステムにおいて、第１コンピュータ装置が、自装置における異常の有無を周期的に監視する監視手段と、前記第２コンピュータ装置宛の電子メールを作成する手段とを備え、前記監視手段が異常を検出する毎に当該異常に関する情報を表す電子メールを作成して前記第２コンピュータ装置に通知することを特徴とする。

【００１１】前記監視手段は、例えば、（１－１）自装置がアクセスする記憶装置の残り容量を監視してその残り容量が予め設定された基準量以下となった場合に異常状態を表す検出情報を作成する資源監視手段、（１－２）自装置の稼働状況を表す履歴情報の変化状態を監視してその変化レベルが予め設定された通知レベルを超える履歴情報を検出したときに異常状態を表す検出情報を作成する履歴情報監視手段、（１－３）自装置における稼働中のプロセス群を予め設定された必要プロセス群情報と不要プロセス群情報とに基づいて特定し、特定したプロセス群に前記必要プロセス群情報及び不要プロセス群情報中に含まれないプロセス或いは不足するプロセスがあるときに異常状態を表す検出情報を作成するプロセス監視手段、（１－４）前記記憶装置に記憶された電子情報の識別子を予め保持した識別情報と比較し、前記識別子が前記識別情報に合致しない場合に異常状態を表す検出情報を作成する識別情報監視手段、の少なくとも一つを周期的に起動し、それぞれ検出情報が出力されたときに前記電子メールを作成するように構成される。

【００１２】また、前記検出情報を所定のＳＭＴＰ対応コードに変換して前記電子メールを作成することを特徴とする。

【００１３】上記他の課題を解決する本発明の異常検出装置は、（２－１）自装置がアクセスする記憶装置の残り容量を監視してその残り容量が予め設定した基準量以下となった場合に異常状態を表す検出情報を作成する資源監視手段、（２－２）自装置の稼働状況を表す履歴情報の変化状態を監視してその変化レベルが予め設定されたレベルを超える履歴情報を検出したときに異常状態を表す検出情報を作成する履歴情報監視手段、（２－３）自装置における稼働中のプロセス群を予め設定された必要プロセス群情報と不要プロセス群情報とに基づいて特定し、前記稼働中のプロセス群に前記必要プロセス群情報及び不要プロセス群情報中に含まれないプロセス或いは不足するプロセスがあるときに異常状態を表す検出情報を作成するプロセス監視手段、（２－４）前記記憶装置に記憶された電子情報の識別子を予め保持した識別情報と比較し、前記識別子が識別情報に合致しない場合に異常状態を表す検出情報を作成する識別情報監視手段、のいずれかを含み、さらに、（２－５）前記検出情報のいずれかが出力されたときに所定形式の電子メールを作成して外部装置に提示する手段、を備えてなる。

【００１４】前記履歴情報監視手段は、例えば、初期稼働時に取得した履歴情報を初期履歴情報として保持し、次回以降の履歴情報が更新された場合に、前記初期履歴情報と前記更新された履歴情報との差分による履歴情報を新たな初期履歴情報として保持するように構成される。

【００１５】上記他の課題を解決する本発明の記録媒体は、記憶装置を具備したコンピュータ装置が読み取り可能なプログラムを記録して成る記録媒体であって、前記プログラムが、下記の処理のいずれかを前記コンピュータ装置に周期的に繰り返し実行させるものであることを特徴とする。（３－１）前記記憶装置の残り容量を監視してその残り容量が予め設定した基準量以下となった場合に異常状態を表す検出情報を作成する処理、（３－２）装置稼働状況を表す履歴情報の変化状態を監視してその変化レベルが予め設定されたレベルを超える履歴情報を検出したときに異常状態を表す検出情報を作成する処理、（３－３）稼働中のプロセス群を予め設定された必要プロセス群情報と不要プロセス群情報とに基づいて特定し、前記稼働中のプロセス群に前記必要プロセス群情報及び不要プロセス群情報中に含まれないプロセス或いは不足するプロセスがあるときに異常状態を表す検出情報を作成する処理、（３－４）前記記憶装置に記憶された電子情報の識別子を予め保持した識別情報と比較し、前記識別子が識別情報に合致しない場合に異常状態を表す検出情報を作成する処理。

【００１６】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を詳細に説明する。

（第１実施形態）図１は、本発明を情報提供を行うコンピュータシステムに適用した場合の実施の形態を表す機能ブロック図である。このコンピュータシステム１は、情報管理サーバ１０と、複数のクライアント２０と、システム全体の統括管理を行うシステム統括管理サーバ３０とを備え、情報管理サーバ１０とシステム統括管理サーバ３０は、公衆網Ｌを介して双方向通信可能に接続されて構成される。

【００１７】情報管理サーバ１０は、汎用のコンピュータ装置と、このコンピュータ装置に読み取られて実行されるコンピュータ・プログラムとで実現されるもので、コンピュータ装置のＯＳは、マルチタスク型のＯＳ、例えばＷｉｎｄｏｗｓＮＴである。この情報管理サーバ１０は、上記コンピュータ・プログラムが実行されることにより形成される、データベース（ＤＢ）１９、リモート管理部１１、WWW、電子メール、Ｐｒｏｘｙ、ＤＮＳ等の処理を行うサーバ機能管理部４１、及び通信管理部４２の機能を備える。リモート管理部１１は、システム資源監視部１３、システムエラー監視部１４、及び不正侵入監視部１５からなるリモート監視部１１と、メッセージ作成部１６と、コード変換部１７と、異常通知部１８とを含んで構成される。

【００１８】なお、上記コンピュータ・プログラムは、通常、上記コンピュータ装置の内部あるいは外部記憶装置に格納され、随時読み取られて実行されるようになっているが、コンピュータ装置とは分離可能な記録媒体、例えばＣＤ－ＲＯＭやＦＤ等に格納され、使用時に上記内部記憶装置または外部記憶装置にインストールされて随時実行に供されるものであってもよい。

【００１９】ＤＢ１９は、サーバ機能管理部４１において用いられる複数の電子情報、情報管理サーバ１０におけるログ、記憶容量の残り容量の比較に用いられ基準量の情報、情報管理サーバ１０の正常稼働時におけるプロセス群リスト情報、情報管理サーバ１０の稼働時において無視可能となるプロセス群リスト情報、及び上記電子情報の識別情報等を格納するものであり、リモート管理部１１（リモート監視部１２）、サーバ機能管理部４１との間で、各々データ授受を行えるように構成されている。

【００２０】リモート管理部１１は、リモート監視部１２で取得される情報管理サーバ１０の運用及び稼働の状態情報、当該状態情報に対応したメッセージの作成、及び当該メッセージの通知を行うものである。このメッセージは、サーバ機能管理部４１、通信管理部４２を介し、さらに公衆網Ｌを通じてシステム統括管理サーバ３０に送られる。

【００２１】リモート監視部１２は、情報管理サーバ１０におけるリソースとなるＤＢ１９の記憶容量、情報管理サーバ１０の運用に関するログ、及び情報管理サーバ１０の稼働状態の監視処理を行う。この監視処理では、後述するシステム資源監視部１３、システムエラー監視部１４、不正侵入監視部１５により、監視情報が周期的に取得される。これらの監視情報は、メッセージ作成部１６に入力され、ここで、対応するメッセージが作成される。

【００２２】リモート監視部１２において、システム資源監視部１３は、情報管理サーバ１０に具備されているＤＢ１９その他の記憶装置に関する記憶容量の監視処理を行うものであり、システムエラー監視部１４は、情報管理サーバ１０における、システムログ、アプリケーションログ、セキュリティログの監視処理を行うものである。ここに「システムログ」とは、情報管理サーバ１０のハードウェア等に関するログであり、「アプリケーションログ」とは、情報管理サーバ１０で稼働するアプリケーションに関するログであり、「セキュリティログ」とは、クライアント２０またはシステム統括管理サーバ３０から情報管理サーバ１０へのアクセスに係る利用者の識別、或いは権限等の情報に関するログである。各監視部１３～１５では、ログが変化した場合に、予め設定された通知レベルを超えるような当該変化の差分について対応する監視情報を作成する。なお、通知レベルは、例えば、上述した３種類のログに対して、その種類毎に、エラーのみ通知または警告とエラーを通知等のように予め設定される。

【００２３】不正侵入監視部１５は、情報管理サーバ１０において、公衆網Ｌを介して不正な侵入者があった場合に、当該侵入行為に対してプロセス管理による監視処理を行うものである。この監視処理は、具体的には、ＤＢ１９中の正常稼働時プロセス群リスト情報と、無視可能プロセス群リスト情報とに基づいて、実際に情報管理サーバ１０で稼働中のプロセス群を前記プロセス群リスト情報と比較することによって行い、当該比較に情報の差異が見られた場合には、対応する監視情報を作成する。

【００２４】無視可能なプロセス群リスト情報には、常駐することなく必要に応じてプロセス自身が稼働を終了するような種類のプロセスが記述されており、不正侵入監視部１５では、この種のプロセスを監視情報作成の対象としないように構成されている。

【００２５】また、不正侵入監視部１５は、ＤＢ１９中に格納されている電子情報の識別情報に対する不正な変更の監視処理を行う。この監視処理は、正しく記述された上記識別情報を保持しておき、情報管理サーバ１０において電子情報の識別情報が不正に変更された場合には、対応する監視情報を作成する。具体的には、電子情報に対するアクセス情報であるＵＲＬ（Uniform Resource Locator）パス名等のフィルタＤＬＬのパス名の正常

値を保持しておき、当該正常値とフィルタＤＬＬのパス名が変更された場合の変更値との比較を行い、当該フィルタＤＬＬのパス名が変更されていると判定された場合には、対応する監視情報を作成する。

【００２６】メッセージ作成部１６は、リモート監視部１２の各機能ブロック１３～１５で入力された監視情報に対応した、システム統括管理サーバ３０へのメッセージを作成する。作成されたメッセージはコード変換部１７に入力される。

【００２７】コード変換部１７は、メッセージ作成部１６から入力されたメッセージをＳＭＴＰに対応したコードのメッセージに変換を行うものである。例えば、ＷｉｎｄｏｗｓＮＴの場合には、使用されている漢字コードは「Ｓ－ＪＩＳ」なので、ＳＭＴＰ対応用のＪＩＳ７に変換される。コード変換されたメッセージは、異常通知部１８に入力される。

【００２８】異常通知部１８は、コード変換部１７で変換されたメッセージを、サーバ機能管理部４１に入力するものである。入力されたメッセージは、サーバ機能管理部４１における電子メール機能を使用し、通信管理部４２を介してシステム統括管理サーバ３０に対して当該メッセージが送信される。

【００２９】次に、本実施形態の情報管理サーバ１０による詳細動作を説明する。図２は、システム資源監視部１３の処理手順図である。システム資源監視部１３は、情報管理サーバ１０に具備されたＤＢ１９における記憶容量の残り容量をチェックして監視情報を作成する（ステップＳ１０１）。残り容量が、ＤＢ１９中に予め設定された基準量情報の基準量より多い場合（ステップＳ１０２：No）、システム資源監視部１３は、予め設定された時間間隔で記憶容量の監視を継続する（ステップＳ１０３）。一方、残り容量が、基準量より少ない場合は（ステップＳ１０２：Yes）、ステップＳ１０１で作成された監視情報に基づいて、メッセージ作成部１６により、システム統括管理サーバ３０へ通知するメッセージを作成する（ステップＳ１０４）。この場合のメッセージは、例えば、基準量を下回ると判定された時刻情報、残り容量情報、当該容量に該当するドライブ名等を含んで作成される。

【００３０】作成されたメッセージは、コード変換部１７により、ＳＭＴＰ対応のコードに変換され（ステップＳ１０５）、異常通知部１８から、サーバ機能管理部４１の電子メール機能を使用して通信管理部４２を介し、ＳＭＴＰ対応のメッセージが送信される（ステップＳ１０６）。当該処理終了後、システム資源監視部１３は、予め設定された時間間隔で記憶容量の監視を継続する（ステップＳ１０７）。

【００３１】図３は、システムエラー監視部１４の処理手順図である。システムエラー監視部１４は、情報管理サーバ１０に具備されたＤＢ１９中に蓄積されるすべてのログをチェックする（ステップＳ２０１）。前回のログと比較して、変化したログが検出されなかった場合（ステップＳ２０２：No）、システムエラー監視部１４は、予め設定された時間間隔でログの監視を継続する（ステップＳ２０３）。変化したログが検出されれば（ステップＳ２０２：Yes）、当該ログと前回ログとの差分情報から監視情報を作成するとともに、当該ログが「システム」、「アプリケーション」、「セキュリティ」のどの種類に属するかを判定する（ステップＳ２０４）。ステップＳ２０４で作成された監視情報中に、予め設定された通知レベルを超えるログがあるか否かをチェックし（ステップＳ２０５）、通知レベルを超えるログを選択するとともに、メッセージ作成部１６により、システム統括管理サーバ３０へ通知するための該当するログに対応したメッセージを作成する（ステップＳ２０６）。

【００３２】作成されたメッセージは、上記ステップＳ１０５～１０６と同様な処理がステップＳ２０７～２０８で施され、ＳＭＴＰ対応のメッセージが送信されるとともに、メッセージに該当するログの監視情報は保存される（ステップＳ２０９）。この監視情報を保存する処理を行うことで、ログに記録される情報は新規情報から構成されるようになる。また、当該処理終了後、システムエラー監視部１４は、予め設定された時間間隔でログの監視を継続する（ステップＳ２１０）。

【００３３】図４は、不正侵入監視部１５の処理手順図である。不正侵入監視部１５では、動作モードのチェックを行い、プロセス監視モードの場合には（ステップＳ３０１：プロセス）、情報管理サーバ１０に稼働中のプロセス群をチェックする（ステップＳ３０２）。当該プロセス群中に、予め設定された無視可能なプロセス群リストに該当するプロセスがある場合には（ステップＳ３０３：Yes）、該当プロセスを無視する（ステップＳ３０４）。また、正常時のプロセス群リストとチェックしたプロセス群とを比較して差異がなければ（ステップＳ３０５：No）、不正侵入監視部１５は、予め設定された時間間隔でログの監視を継続する（ステップＳ３０６）。差異があれば（ステップＳ３０５、Yes）、当該差異情報から監視情報を作成し、メッセージ作成部１６により、システム統括管理サーバ３０へ通知する当該監視情報に対応したメッセージを作成する（ステップＳ３０７）。作成されたメッセージは、上記ステップＳ１０５～１０６と同様な処理がステップＳ３０８～３０９で施され、ＳＭＴＰ対応のメッセージが送信されるとともに、当該処理終了後、不正侵入監視部１５は、予め設定された時間間隔でログの監視を継続する（ステップＳ３１０）。

【００３４】一方、動作モードが電子情報の識別情報変更監視モードの場合には（ステップＳ３０１：識別情報）、現在のフィルタＤＬＬのパス名をチェックする

（ステップＳ３１１）。当該ＤＬＬのパス名と予め設定されたフィルタＤＬＬのパス名の正常パス名とが同一であれば（ステップＳ３１２、Yes）、不正侵入監視部１５は、予め設定された時間間隔でログの監視を継続する（ステップＳ３１３）。同一でなければ（ステップＳ３１２、No）、上記ステップＳ３０７～３０９と同様な処理が施される。当該処理終了後、不正侵入監視部１５は、予め設定された時間間隔で識別情報の変更の監視を継続する（ステップＳ３１８）。

【００３５】なお、情報管理サーバ１０では、例えば、リモート監視部１２における監視時間間隔等のシステムパラメータの設定に、ＷｉｎｄｏｗｓＮＴのレジストリ機能を使用することにより、設定パラメータをシステム統括管理サーバ３０から情報管理サーバ１０に対して動的な更新を行うようにしている。

【００３６】このように、本実施形態のコンピュータシステム１では、情報管理サーバ１０が、正常時に稼働するプロセス群リストと稼働しても無視可能なプロセス群リストとを予め具備してプロセス管理を行うので、プロセスの必要・不要の判定が自動的に行われる。また、情報管理サーバ１０がアクセスするディスク等の記憶容量に対して、予め設定された基準量と実際の残り記憶容量とを比較するので、容量の減少に伴う動作の不具合原因を検出できる。さらに、プロセス管理により、不要プロセスの発生や、必要プロセスの消失等に関する検出が可能なことから、システムに不正に侵入された場合には、プロセスの状態から当該侵入行為の検出が可能となる。

【００３７】情報管理サーバ１０では、また、システム統括管理サーバ３０に通知するメッセージの漢字コードをS-ＪＩＳコードからＪＩＳ７に変換してＳＭＴＰ対応のコード変換による電子メール送信を行うので、ＷｉｎｄｏｗｓＮＴのＰＣ環境において、他の電子メールシステムとの互換性を提供することができ、また、フィルタＤＬＬのパス名の正常値を予め保持しておき、ＤＬＬのパス名が変更された場合には検出して通知することにより、不正なＤＬＬのパスの変更に対して監視が可能になる。また、情報管理サーバ１０ではシステムパラメータの設定に、ＷｉｎｄｏｗｓＮＴのレジストリ機能を採用することにより、システム統括管理サーバ３０から情報管理サーバ１０に対して設定パラメータの変更処理等を公衆網を介したリモート環境で動的な制御が可能となる。

【００３８】また、情報管理サーバ１０が自己サイトのログに関する情報、及び異常や障害等に関する情報等をシステム統括管理サーバ３０に通知するので、システム統括管理サーバ３０は、情報管理サーバ１０に対してリモートアクセスすることなく、ログの取得、及び検査が可能になるとともに、定期的な管理が不要になり、また、情報管理サーバ１０が再度起動不可能となるような、重大なシステム障害が発生した場合でも、当該障害に至るまでの経緯を取得（把握）することができる。

【００３９】（第２実施形態）本発明は、スタンドアロン型のコンピュータ装置を用いた異常検出装置として実施することも可能である。この場合の異常検出装置は、スタンドアロン型のコンピュータ装置の内部あるいは外部記憶装置に構築されるＤＢ１９を備え、さらに、上記コンピュータシステム１の情報管理サーバ１０と同一の機能ブロックである、システム資源監視部１３、システムエラー監視部１４、不正侵入監視部１５、メッセージ作成部１６、コード変換部１７、及び異常通知部１８、を具備して構成される。

【００４０】この異常検出装置が情報管理サーバ１０と相違する点は、異常検出装置に情報を提示するための表示装置を備える点、リモート管理部１１、リモート監視部１２、及び通信管理部４２の機能ブロックを具備しない点であり、通信管理部４２に相当する処理は、異常検出装置に具備されるディスプレイ装置等の出力装置に対してメッセージの出力を行うように異常通知部１８を構成させることで代替が可能となる。この異常検出装置では、記憶容量監視、ログ監視、及びプロセス監視により、上記情報管理サーバ１０と同様な効果を得ることが可能となる。

【００４１】

【発明の効果】以上の説明から明らかなように、本発明によれば、情報管理サーバの稼働及び運用に関する監視を行うことにより、ディスク等の記憶容量の減少に伴う稼働状況の不具合を事前に防ぐとともに、異常が検出された場合に、電子メールを使用して外部の情報管理サーバ等に通知することにより、特定の情報管理サーバが完全に故障した場合でも、当該故障に至った経緯をログとして解析することが可能となり、システム全体の信頼性及び運用管理が格段に向上する効果がある。

【図面の簡単な説明】

【図１】本発明のコンピュータシステムの一実施形態を表す機能ブロック図。

【図２】システム資源監視部における処理手順図。

【図３】システムエラー監視部における処理手順図。

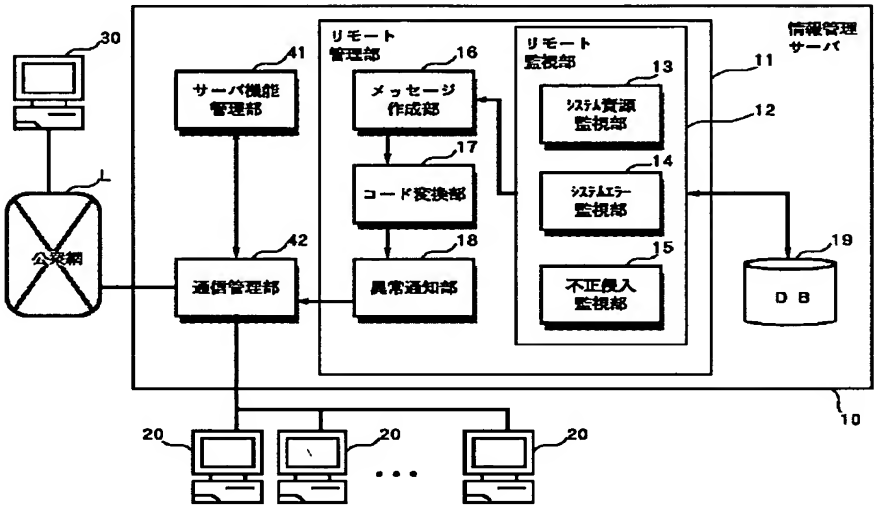
【図４】不正侵入監視部における処理手順図。

【符号の説明】

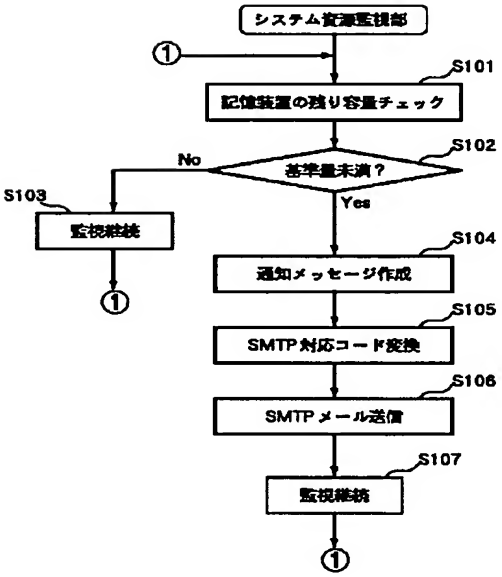
１　コンピュータシステム
１０　情報管理サーバ
１１　リモート管理部
１２　リモート監視部
１３　システム資源監視部
１４　システムエラー監視部
１５　不正侵入監視部
１６　メッセージ作成部
１７　コード変換部
１８　異常通知部
１９　データベース（ＤＢ）

２０　クライアント
３０　システム統括管理サーバ
４１　サーバ機能管理部
４２　通信管理部

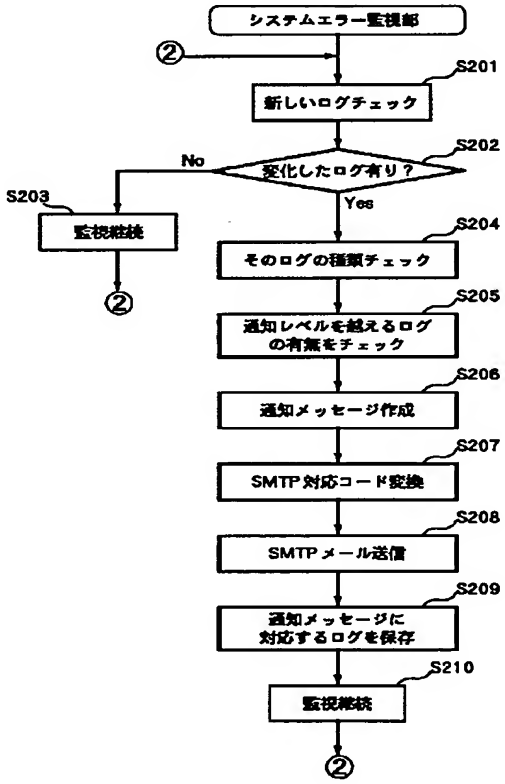
【図１】



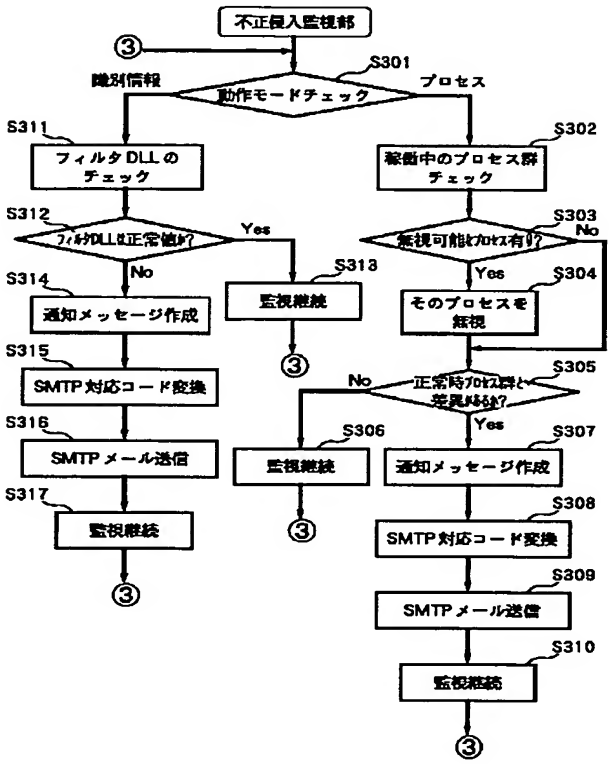
【図２】



【図３】



【図４】


不正侵入監視部
③
S301
識別情報
動作モードチェック
プロセス
S311
フィルタDLLのチェック
S302
稼働中のプロセス群チェック
S312
フィルタDLLは正常値か?
Yes
No
S303
無視可能プロセス有り?
No
Yes
S313
監視継続
S304
そのプロセスを無視
S314
通知メッセージ作成
③
S315
SMTP対応コード変換
No
正常時プロセス群と差異有り?
S305
S316
SMTPメール送信
Yes
S306
監視継続
S307
通知メッセージ作成
S317
監視継続
③
③
S308
SMTP対応コード変換
S309
SMTPメール送信
S310
監視継続
③